UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

PAMELA SMITH, on behalf of herself and all others similarly situated, Plaintiff, v. ALVARIA, INC. and CARRINGTON MORTGAGE SERVICES, LLC, Defendants.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Pamela Smith brings this Class Action Complaint ("Complaint") against Carrington Mortgage Services, LLC ("CMS") and Alvaria, Inc. ("Alvaria") (collectively, "Defendants"), as an individual and on behalf of all others similarly situated, and alleges upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard Plaintiff's and other similarly situated CMS customers' ("Class Members") personally identifiable information ("PII" or "Private Information"), including full names, telephone numbers, loan numbers and balances, mailing addresses, and last four digits of Social Security numbers, from unauthorized disclosure to cybercriminals.[1]

2. Defendant CMS is a fully integrated mortgage company with lending and servicing

[1] *See* https://nextmortgagenews.com/news/tech-vendor-names-carrington-in-data-breach-notice/ (last visited on May 17, 2023).

operations.[2] Headquartered in California, CMS services loans in all fifty (50) states and Puerto Rico and is licensed to lend in 48 states.[3]

3. Alvaria touts itself as a "global leader delivering optimized customer experience and workforce engagement software and cloud service technology solutions, "help[ing] companies create better experiences for their customers and employees who serve them."[4]

4. Plaintiff brings this class action lawsuit to address Defendants' collective inadequacies in the safeguarding and supervision of Class Members' Private Information, including, but not limited to, Defendants' failure to comply with industry standards to protect Plaintiff's and Class Members' Private Information and to provide adequate notice to Plaintiff and Class Members that their PII had been compromised following the March 9, 2023 attack on Alvaria's customer environment (the "Data Breach").

5. Plaintiff seeks, among other things, orders requiring Defendants to fully and accurately disclose the nature of the information that was compromised and to adopt sufficient security practices and safeguards to prevent incidents like the Data Breach from occurring again in the future.

6. Plaintiff and Class Members would not have provided their Private Information to Defendants if they had known that Defendants would breach their obligations, privacy promises, and agreements by (a) failing to ensure that they had adequate data security measures in place to protect the Private Information from compromise and exfiltration, and/or (b) knowingly providing Plaintiff's and Class Members' Private Information to a vendor that utilized inadequate security

[2] *See* https://www.carringtonmortgage.com/our-mission (last visited on May 7, 2023).
[3] *Id.*
[4] *See* https://www.alvaria.com/companv/about-alvaria (last visited on May 7, 2023).

measures.

7. Armed with the Private Information accessed in the Data Breach, data thieves can and will commit a variety of crimes against Plaintiff and Class Members, including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

8. There has been no assurance offered by Defendants that all personal data or copies of data have been recovered or destroyed, or that Defendants have adequately enhanced their data security practices sufficient to avoid a similar breach of their network in the future.

9. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, including out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

10. Plaintiff brings this class action lawsuit to address Defendants' inadequate safeguarding and supervision of Class Members' Private Information that they collected and maintained. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to Defendants, thus Defendants were on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

11. Upon information and belief, Defendants and their employees and vendors failed to properly monitor the computer network and systems that housed the Private Information. Had

they properly monitored their networks and provided adequate supervision over their agents, vendors, and/or suppliers, the Data Breach could have been prevented.

12. Plaintiff's and Class Members' identities are now at risk because of Defendants' negligent conduct as the Private Information that Defendants collected and maintained is now in the hands of data thieves and other unauthorized third parties.

13. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

II. PARTIES

14. Plaintiff Pamela Smith is, and at all times mentioned herein was, an individual citizen of the State of Illinois.

15. Defendant Alvaria, Inc. is a business software company incorporated in Delaware, with its principal place of business at 5 Technology Park Dr, Westford, Massachusetts 01886, in Middlesex County.

16. Defendant CMS is a fully integrated mortgage company headquartered at 1600 South Douglass Road, Suites 110 & 200-A, in Anaheim, California 92806, in Orange County.

III. JURISDICTION AND VENUE

17. This Court has jurisdiction over the parties and the subject matter of this action. Jurisdiction is proper because Defendant Alvaria is a corporation operating throughout the nation whose principal place of business is in the Commonwealth of Massachusetts and because CMS conducts business in and has sufficient minimum contacts with the Commonwealth of Massachusetts, including but not limited to, through its sharing of members' personal information with Alvaria and contracting with Alvaria regarding the safekeeping of personal information.

18. This Court has diversity jurisdiction over this action under the Class Action

Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many class members, including Plaintiff, are citizens of states that differ from Defendant.

19. Venue is proper in this District because the acts and omissions complained of herein occurred (and Defendant Alvaria is located) within this District. Upon information and belief. Plaintiff's and Class Members' Private Information was also being maintained within this District.

IV. FACTUAL ALLEGATIONS

A. Defendants' Business

20. Founded in 2007, CMS is a fully integrated mortgage company with lending and servicing operations throughout the country. In fact, CMS services loans in all fifty (50) states and Puerto Rico and is licensed to lend in 48 states.

21. Alvaria is a workforce management and call center technology solution headquartered in Massachusetts.[5]

22. As a condition of receiving loan servicing and other mortgaging services, CMS requires that its customers turn over highly sensitive personal information.

23. In its "Privacy Policy," CMS makes clear that it "do[es] not rent, sell, or share with third parties the Personal Information [it] collect[s]" from its customers except for in the case of "third party vendors" engaged to provide services on CMS' behalf, "such as hosting, web-site development, and support, have access to Personal Information."[6]

[5] *See* https://www.alvaria.com/conipanv/about-alvaria (last visited on May 7, 2023).
[6] *See* https://www.carringtonmortgage.com/legal/privacv-policv (last visited on May 7, 2023).

24. Importantly, CMS acknowledges in the Privacy Policy that its vendors, including Alvaria, "have agreed not to disclose the Personal Information or to use it for any purpose other than providing the requested services."[7]

25. In Alvaria's Privacy Policy, it promises to only share Plaintiff's and Class Members' Private Information "if such disclosure is in accordance with this Privacy Policy and provided that it is lawful to do so."[8]

26. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants also assumed legal and equitable duties owed to them and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

27. Plaintiff and Class Members relied on Defendants to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendants ultimately failed to do.

28. Plaintiff and Class Members would not have allowed Defendants to maintain their Private Information absent Defendants' agreement to keep that information secure from disclosure.

B. The Data Breach

29. On November 28, 2022, the Hive Ransomware group executed a ransomware attack on Alvaria's internal corporate network; shortly thereafter, on December 21, 2022, criminal actors released certain corporate records onto the dark web.

30. Subsequently, on March 9, 2023, Alvaria failed to prevent a second attack on a

[7] *Id.*

[8] *See* https://www.alvaria.com/legal/privacy-policy (last visited on May 7, 2023).

portion of its customer environment that maintained Plaintiff's and Class Members' Private Information.

31. Despite the November 28, 2022 data breach, Defendant CMS nevertheless continued to utilize Alvaria's services as its vendor and allowed it to maintain its customers' personal information.

32. On information and belief, CMS failed to properly audit or determine Alvaria's cybersecurity practices following the November 28, 2022 data breach.

33. Through the subsequent Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including loan information, mailing addresses, and the last four digits Social Security numbers.

34. Alvaria delivered Notices of Data Incident letters to Plaintiff and Class Members, alerting them that their highly sensitive Private Information had been exposed.

35. Defendants had obligations created by contract, industry standards, common law, federal and state regulations, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

36. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such Information confidential and secure from unauthorized access.

C. Defendants Failed to Comply with FTC Guidelines

37. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-

making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC V. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

38. In October 2016, the FTC updated its publication. *Protecting Personal Information: A Guide for Business,* which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

39. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

40. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

41. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

42. Defendants were at all times fully aware of their obligation to protect the Private Information of Plaintiff and Class Members but failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so.

D. Defendants Failed To Comply With Industry Standards

43. As noted above, experts studying cyber security routinely identify entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

44. Several best practices have been identified that at a minimum should be implemented by companies in possession of Private Information, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

45. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible

communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

46. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

47. The foregoing frameworks are existing and applicable industry standards for a company's obligations with respect to data privacy. Upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

E. Defendants Breached Their Duty to Safeguard Consumers' Private Information

48. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols (and those of their business associates, vendors, and/or suppliers) adequately protected the Private Information of Class Members.

49. Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their

computer systems and data (or, in the case of CMS, those of its vendor, Alvaria). Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to adequately protect Plaintiff's and Class Members' Private Information;

b. Failing to sufficiently train and/or monitor their employees and/or vendors regarding the proper handling of Plaintiff's and Class Members' Private Information;

c. Failing to fully comply with FTC guidelines for cybersecurity, in violation of the FTCA; and

d. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' Private Information.

50. Had Defendants remedied the deficiencies in their information storage and security practices, procedures, and protocols, followed industry guidelines, and adopted security measures recommended by experts in the field, they could have prevented the theft of Plaintiff's and Class Members' confidential Private Information.

51. Accordingly, Plaintiff's and Class Members' lives were severely disrupted.

52. In addition, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft.

F. Defendants Should Have Known that Cybercriminals Target PII to Carry Out Fraud and Identity Theft

53. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store Private Information, like Defendants, preceding the date of the breach.

54. Data breaches, including those perpetrated against companies that store Private

Information in their systems, have become widespread.

55. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[9]

56. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[10]

57. Defendants knew and understood that unprotected or exposed Private Information in the custody of companies, like Defendants, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

58. In light of recent high profile data breaches at industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

59. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[11]

---

[9] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

[10] *Id.*

[11] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted- ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last

60. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

61. A ransomware attack, like that experienced by Defendants is a type of cyberattack that is frequently used to target companies due to the sensitive data they maintain.[12] In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[13]

62. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[14] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

63. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[15] In 2020, over 50% of ransomware attackers exfiltrated data from a network

---

accessed Oct. 17, 2022).

[12] *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/

[13] *Ransomware FAQs*, available at https://www.cisa.gov/stopransomware/ransomware-faqs

[14] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends

[15] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/

before encrypting it.[16] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[17] And even where companies pay for the return of data, attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[18]

64. In light of the above, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industries, including Defendants.

65. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

66. In the Notice Letter, Defendants make an offer of 24 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

G. The Consequences of a Data Breach are Long Lasting and Severe

67. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[19]

---

[16] 2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020- ransomware-marketplace-report

[17] *Id.*

[18] *Id.*

[19] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission,

(October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-

68. Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

69. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

70. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

71. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

72. One such example of criminals piecing together bits and pieces of compromised

---

workshop-be-bcp-staff- perspective/informational injury workshop staff report-oct 2018 0.pdf (last visited on April 28, 2023).

PII for profit is the development of "Fullz" packages.[20]

73. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

74. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

75. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and Class Members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

76. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' compromised Private

[20] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm,* Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance- finn/ (last visited on May 7, 2023).

Information to access accounts, including, but not limited to, email accounts and financial accounts, in order to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

77. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[21]

78. However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

79. Identity thieves can also use stolen personal information such as Social Security numbers (or even the last four digits of an individual's Social Security number)[22] for a variety of crimes.

80. Indeed, scammers only need the last four digits of a Social Security number coupled with other PII to commit fraud, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief s picture, to obtain government and/or medical benefits, or to file a fraudulent tax return using the victim's information.[23]

---

[21] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitvtheft.gov/Steps (last visited April 28, 2023).

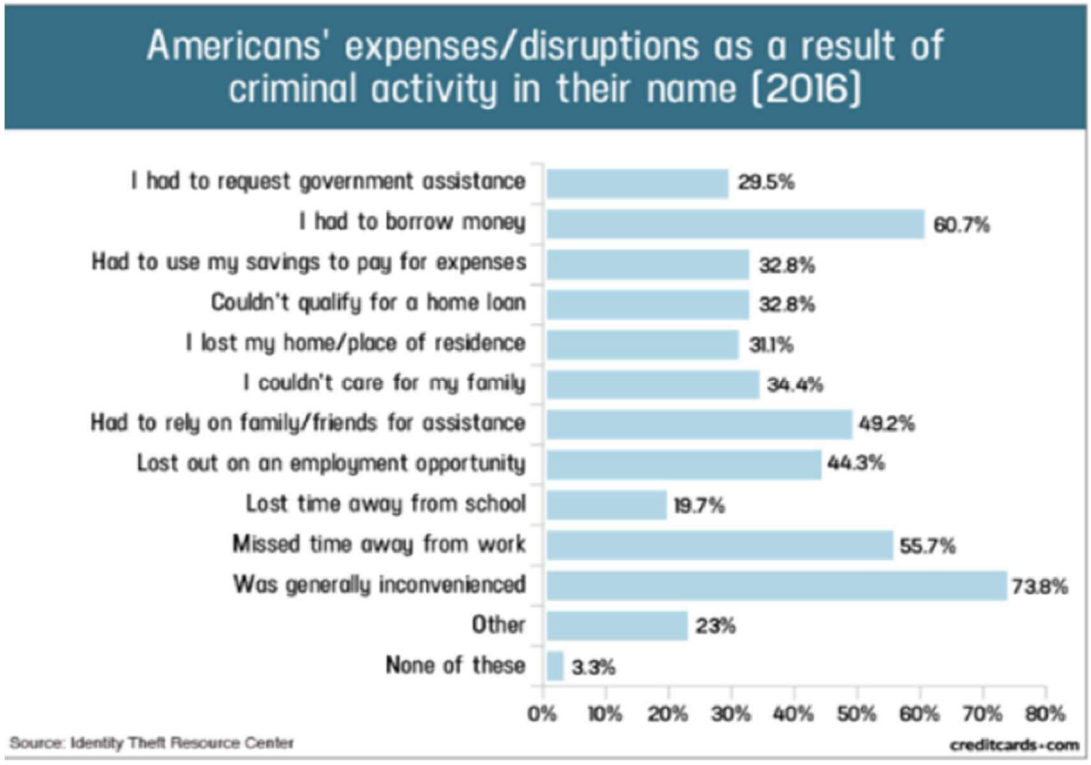
[22] *See* https://www.eamcheese.com/post/the-last-4-digits-of-vour-ssn#:~:text=As%201ong%20as%20a%20hacker.tax%20refunds%20in%20vour%20name (last visited on May 7, 2023).

[23] *See* https://consumerboomer.com/what-can-a-scammer-do-with-the-last-4-digits-of-vour-social/ (last visited on May 7, 2023).

81. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

82. Even with the last four digits of a Social Security number, cybercriminals can easily use complex computer algorithms to guess the remaining five digits.[24]

83. In fact, a study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of PII:[25]



84. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data

[24] *See* "Social Security Numbers Are Easy to Guess," https://www.science.org/content/article/social- security- numbers-are-easy-guess (last visited on May 7, 2023).

[25] Steele, Jason, *Credit Card and ID Theft Statistics,* CreditCards.com (October 23, 2017), *available at* https://www. creditcards.com/credit-card-news/credit-card-securitv-id-theft-fraud-statistics-1276/ (last visited on April 28, 2023).

breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[26]

85. Here, the last four digits of Social Security numbers were compromised (along with other highly sensitive PII). The value of such PII is axiomatic. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

86. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:'[27]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

87. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

88. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future and have no choice but to vigilantly monitor their accounts for many years to come.

F. Plaintiff's and Class Members' Damages

89. Plaintiff and Class Members, as customers of CMS, have been damaged by the

---

[26] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").

[27] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited April 28, 2023).

compromise of their Private Information in the Data Breach.

90. Plaintiff and Class Members entrusted their Private Information to Defendants in order to receive Defendants' services.

91. Plaintiff's Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendants' inadequate data security practices, procedures, and protocols, as discussed herein.

92. As a direct and proximate result of Defendants' actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility accounts opened in their names, credit card accounts opened in their names, and other forms of identity theft.

93. Further, as a direct and proximate result of the Data Breach, Plaintiff and Class Members have been forced to expend time dealing with and attempting to mitigate the negative effects thereof.

94. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

95. The Private Information targeted and stolen from Defendants' system, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against them.

96. Additionally, Plaintiff and Class Members have spent and will continue to spend

significant amounts of time monitoring their accounts and records, including medical records and explanations of benefits, for misuse.

97. Plaintiff and Class Members were also injured by and suffered benefit-of-the-bargain damages from this Data Breach. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not.

98. Part of the price Plaintiff and Class Members paid to Defendants was intended to be used by Defendants to fund adequate security of their computer systems and networks and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and Class Members did not get what they paid for and agreed to.

99. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.[28]

100. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[29,30] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[31]

101. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release.

102. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private

---

[28] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[29] https://datacoup.com/

[30] https://digi.me/what-is-digime/

[31] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

103. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

104. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Placing "freezes" and "alerts" with credit reporting agencies;

f. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

g. Contacting financial institutions and closing or modifying financial accounts;

h. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

j. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

105. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Defendants and their

business associates, vendors, and/or suppliers, is protected from future breaches by the implementation of more adequate data security measures and safeguards.

106. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

G. Plaintiff Smith's Experience

107. Plaintiff Smith has a mortgage through CMS. When Plaintiff applied and received her mortgage loan, she was required to provide extensive amounts of her PII to CMS, including her name and Social Security number.

108. At the time of the Data Breach (March 9, 2023), Defendants retained Plaintiff's PII in their systems.

109. Plaintiff Smith is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. In addition, she has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

110. Plaintiff Smith received the Notice Letter directly from Defendants. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties. This sensitive information included Plaintiff's name, mailing address, phone number, loan information, and the last four digits of her Social Security number.

111. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach including, but not limited to, setting up a new email address and researching and signing up for the credit monitoring and identity theft protection services offered by Defendant. Plaintiff has spent approximately fifty hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be

recaptured.

112. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (a) invasion of privacy (b) diminution in the value of her PII, a form of property that Defendants obtained from Plaintiff; (c) lost time, spent remedying the harms resulting from the Data Breach; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

113. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants has still not fully informed her of key details about the Data Breach's occurrence.

114. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

115. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

116. Plaintiff Smith has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

117. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Fed. R. Civ. P. 23.

118. Specifically, Plaintiff proposes the following Nationwide Class (also referred to herein as the "Class"), subject to amendment as appropriate:

Nationwide Class

All persons residing in the United States who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

119. Plaintiff proposes the following Illinois Subclass (also referred to herein as the "Illinois Subclass" or "Subclass"), subject to amendment as appropriate:

Illinois Subclass

All persons residing in the state of Illinois who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

120. Excluded from the Class and Subclass are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

121. Plaintiff reserves the right to modify or amend the definition of the proposed Classes and/or add subclasses before the Court determines whether certification is appropriate.

122. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact identities of Class Members are unknown at this time, based on information and belief, the Class consists of roughly 3,037,303 individuals whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Defendants' records. Class Members' records, publication notice, self-identification, and other means.

123. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants engaged in the conduct alleged herein;

b. Whether Defendants' conduct violated the FTCA;

c. Whether and to what extent Defendants had a duty to protect the Private Information of Class Members;

d. When Defendants learned of the vulnerability within Alvaria's network that led to the Data Breach;

e. Whether Defendants' response to the Data Breach was adequate;

f. Whether Defendants took reasonable steps and measures to safeguard Plaintiff's and Class Members' Private Information;

g. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

h. Whether hackers obtained Class Members' Private Information via the Data Breach;

i. Whether Defendants knew or should have known that their data monitoring and supervision processes were deficient;

j. Whether Defendants were aware that their business associates,' vendors,' and/or suppliers' data security practices, procedures, and protocols were inadequate;

k. What damages Plaintiff and Class Members suffered as a result of Defendants' misconduct;

l. Whether Defendants' conduct was negligent;

m. Whether Defendants were unjustly enriched;

n. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

o. Whether Plaintiff and Class Members are entitled to lifetime credit or identity

monitoring and monetary relief; and

p. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

124. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia,* all Class Members were injured through the common misconduct of Defendants. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

125. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

126. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way and as a result of the same negligent acts and omissions committed by Defendants. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

127. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered

in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

128. Defendants have acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

129. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE CLASSES)

130. Plaintiff restates and realleges all of the allegations in paragraphs 1-129 as if fully set forth herein.

131. Defendants knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in

safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

132. Defendants knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security.

133. Defendants were on notice because, on information and belief, they knew or should have known that the Private Information would be an attractive target for cyberattacks.

134. Defendants owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to them. Defendants' duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, supervising, monitoring, and protecting the Private Information in their possession;

b. To protect members' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in their possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

135. Defendants' duty to employ reasonable data security measures arose, in part,

under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair. . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

136. Defendants' duty also arose because Defendants were bound by industry standards to protect their respective customers' confidential Private Information entrusted to them.

137. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendants and their associates, vendors, and/or suppliers, and Defendants owed them a duty of care to not subject them to an unreasonable risk of harm.

138. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within their care.

139. Defendants, by their actions and/or omissions, breached their duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate data security practices to safeguard the Private Information of Plaintiff and Class Members.

140. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information.

141. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of the Private Information;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to comply with the FTCA; and

e. Failing to comply with other state laws and regulations, as further set forth herein.

142. Defendants had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Defendants with their Private Information was predicated on the understanding that Defendants would take adequate security precautions.

143. Defendants' breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised, exfiltrated, and misused, as alleged herein.

144. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the industry.

145. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

146. As a result of Defendants' ongoing failure to notify Plaintiff and Class Members regarding exactly what Private Information has been compromised, Plaintiff and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

147. Defendants' breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

148. As a result of Defendants' negligence in breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent

purposes.

149. Defendants also had independent duties under state laws that required them to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

150. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

151. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

152. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

153. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia,* strengthen their data security monitoring procedures, conduct periodic audits of those procedures, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
BREACH OF CONTRACT
(AGAINST CMS ON BEHALF OF PLAINTIFF AND THE CLASSES)

154. Plaintiff restates and realleges all of the allegations in paragraphs 1-129 as if fully set forth herein.

155. Plaintiff and Class Members entered into valid and enforceable contracts through which they were required to turn over their Private Information to CMS in exchange for services. That contract included promises by CMS to secure, safeguard, and not disclose Plaintiff's and Class Members' Private Information to any third parties without their consent.

156. CMS's Privacy Policy memorialized the rights and obligations of CMS and its

customers. This document was provided to Plaintiff and Class Members in a manner in which it became part of the agreement for services.

157. In its Privacy Policy, CMS commits to protecting the privacy and security of the Private Information and promises to never share Plaintiff's and Class Members' Private Information except under certain limited circumstances.

158. Plaintiff and Class Members fully performed their obligations under their contracts with CMS. However, CMS failed to secure, safeguard, and/or keep private Plaintiff's and Class Members' Private Information, and therefore CMS breached its contracts with Plaintiff and Class Members.

159. Despite its knowledge of Alvaria's previous lax data security measures that led to at least one previously known data breach in November of 2022, CMS allowed Alvaria to maintain possession and control of Plaintiff's and Class Members' Private Information, leading to criminal third parties' accessing, copying, and/or exfiltrating Plaintiff's and Class Members' Private Information without permission through CMS's failure to adequately vet and supervise Defendant Alvaria. Therefore, CMS breached its contracts with Plaintiff and Class Members.

160. CMS's failure to satisfy its confidentiality and privacy obligations resulted in CMS providing services to Plaintiff and Class Members that were of a diminished value and in breach of its contractual obligations to Plaintiff and Class Members.

161. As a result. Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein, including by CMS's failure to fully perform its part of the agreement with Plaintiff and Class Members.

162. Asa direct and proximate result of CMS's conduct, Plaintiff and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

163. In addition to monetary relief. Plaintiff and Class Members are also entitled to injunctive relief requiring CMS to, *inter alia,* strengthen its data security monitoring and supervision procedures, conduct periodic audits of those procedures, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(AGAINST CMS ON BEHALF OF PLAINTIFF AND THE CLASSES)

164. Plaintiff restates and realleges all of the allegations in paragraphs 1-129 as if fully set forth herein.

165. This Count is pleaded in the alternative to Count II above.

166. CMS provides mortgage services to Plaintiff and Class Members. Plaintiff and Class Members formed an implied contract with CMS regarding the provision of those services through its collective conduct, including by Plaintiff and Class Members providing their Private Information to CMS in exchange for the services offered.

167. Through CMS's offering of these services, it knew or should have known that it needed to protect Plaintiff's and Class Members' confidential Private Information in accordance with its own policies, practices, and applicable state and federal law.

168. As consideration, Plaintiff and Class Members turned over valuable Private Information to CMS. Accordingly, Plaintiff and Class Members bargained with CMS to securely maintain and store their Private Information.

169. CMS accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services, including data security, to Plaintiff and Class Members.

170. In delivering their Private Information to CMS in exchange for its services, Plaintiff and Class Members intended and understood that CMS would adequately safeguard the

Private Information as part of those services.

171. CMS's implied promises to Plaintiff and Class Members include, but are not limited to: (1) taking steps to ensure that anyone who is granted access to Private Information, including its business associates, vendors, and/or suppliers, also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its business associates, vendors, and/or suppliers is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees, business associates, vendors, and/or suppliers; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

172. Plaintiff and Class Members would not have entrusted their Private Information to CMS in the absence of such an implied contract.

173. Had CMS disclosed to Plaintiff and the Class that it did not have adequate data security and data supervisory practices to ensure the security of their sensitive data, including but not limited to CMS's decision to continue to entrust Plaintiff's and Class Members' Private Information to Alvaria despite Alvaria's November 2022 data breach, Plaintiff and Class Members would not have provided their Private Information to CMS.

174. As providers of lending and mortgage servicing operations, CMS recognized (or should have recognized) that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiff and the Class.

175. CMS violated these implied contracts by failing to employ reasonable and

adequate security measures and supervision of its vendors, business associates, and/or suppliers to secure Plaintiff's and Class Members' Private Information.

176. A meeting of the minds occurred, as Plaintiff and Class Members agreed, *inter alia,* to provide accurate and complete Private Information to CMS in exchange for CMS's agreement to, *inter alia,* protect their Private Information.

177. Plaintiff and Class Members have been damaged by Defendants' conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT IV
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(AGAINST ALVARIA ON BEHALF OF PLAINTIFF AND THE CLASSES)

178. Plaintiff restates and realleges all of the allegations in paragraphs 1-129 as if fully set forth herein.

179. Alvaria is a workforce management and call center technology solution company.

180. Alvaria entered into a contract with CMS in which it promised not to ever disclose Plaintiff's and Class Members' Private Information or to use it for any purpose other than the services requested by CMS.

181. This contract was made expressly for the benefit of Plaintiff and the Class, as it was their Private Information that Alvaria agreed to collect and promised CMS it would protect.

182. Alvaria knew that if it were to breach this contract with CMS, then CMS's customers, including Plaintiff and Class Members, would be harmed.

183. Alvaria breached its contract with CMS when it failed to use reasonable data security measures, including those in compliance with the FTCA and industry standards, that could have prevented the Data Breach.

184. As foreseen, Plaintiff and the Class were harmed by Alvaria's breach, as set forth herein.

185. Accordingly, Plaintiff and Class Members are entitled to damages in an amount to be determined at trial, along with their costs and attorney's fees incurred in this action.

COUNT V
VIOLATION OF ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
815 ILCS § 505/1 et seq.
(ON BEHALF OF PLAINTIFF AND THE ILLINOIS SUBCLASS)

186. Plaintiff incorporates all previous paragraphs as if fully set forth below.

187. The Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS § 530/20 provides that a violation of that statute constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 § et seq. ("ICFA"), which prohibits unfair and deceptive acts or practices in the conduct of trade and commerce.

188. Defendants are "data collectors" under IPIPA. As data collectors, Defendants own or license information concerning Illinois residents.

189. The IPIPA requires a data collector that "maintains or stores . . . records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, . . . use, . . . or disclosure." IPIPA, 815 ILCS § 530/45(a).

190. The IPIPA further requires that data collectors "notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system." (emphasis added).

191. As alleged above, Defendants violated the IPIPA by failing to implement and maintain reasonable security measures to protect Plaintiff and members of the Illinois Subclass's PHI and PII. Defendants further violated the IPIPA by failing to give Plaintiff and members of the Illinois Subclass expedient notice without unreasonable delay.

192. As a direct and proximate cause of Defendants' failures, Plaintiff and members of the Illinois Subclass have suffered actual damages.

193. Plaintiff, on behalf of herself and the Illinois Subclass, seeks compensatory damages for breach of the IPIPA and the ICFA, which include, but are not limited to, the costs of future monitoring of their credit history for identity theft and fraud, plus attorney's fees, prejudgment interest, and costs.

COUNT VI
UNJUST ENRICHMENT / QUASI CONTRACT
(ON BEHALF OF PLAINTIFF AND THE CLASSES)

194. Plaintiff restates and realleges all of the allegations in paragraphs 1-129 as if fully set forth herein.

195. Plaintiff brings this count in the alternative the contract counts above.

196. Plaintiff and Class Members conferred a benefit on Defendants. Specifically, they provided Defendants with their Private Information, which Private Information has inherent value. In exchange. Plaintiff and Class Members should have been entitled to Defendants' adequate protection and supervision of their Private Information, especially in light of their special relationship.

197. Defendants knew that Plaintiff and Class Members conferred a benefit upon them and have accepted and retained that benefit by accepting and retaining the Private Information entrusted to them. Defendants profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

198. Defendants failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

199. Defendants acquired the Private Information through inequitable record retention as it failed to disclose the inadequate data security practices, procedures, and protocols previously alleged.

200. If Plaintiff and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to secure their Private Information, they would have made alternative mortgage servicing choices that excluded Defendants.

201. Plaintiff and Class Members have no adequate remedy at law.

202. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon them.

203. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct alleged herein. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

204. Plaintiff and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining

the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendants to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Defendants to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all triable issues.

DATED: May 30, 2023

Respectfully submitted,

/s/ David Pastor

David Pastor, BBO #391000
PASTOR LAW OFFICE, PC
63 Atlantic Avenue, 3rd Floor
Boston, MA 02110
Phone: 617-742-9700
Fax: 617-742-9701
Email: dpastor@pastorlawoffice.com

Christopher D. Jennings*
Tyler B. Ewigleben*
THE JOHNSON FIRM
610 President Clinton Ave., Suite 300
Little Rock, AR 72201
Tel: (501) 372-1300
Email: chris@yourattorney.com
Email: tyler@yourattorney.com

Attorneys for Plaintiff and the Proposed Class

*PRO HAC VICE FORTHCOMING